2014

Meatspace, the Internet, and the Cloud: How Changes in Document Storage and Transfer Can Affect IP Rights

Sharon Sandeen
Mitchell Hamline School of Law, sharon.sandeen@mitchellhamline.edu

Publication Information
12 DePaul Business & Commercial Law Journal 437 (2014)

Meatspace, the Internet, and the Cloud: How Changes in Document Storage and Transfer Can Affect IP Rights

Abstract
This article discusses the intellectual property issues from "meatspace" to online services and the Internet. It further explores intellectual property issues from the Internet to the Cloud. Finally, it discusses the implications of cloud computing for trade secret protection.

Keywords
cloud computing, internet, cyberspace, trade secrets

Disciplines
Computer Law | Intellectual Property Law

Meatspace, the Internet, and the Cloud: How Changes in Document Storage and Transfer Can Affect IP Rights

Sharon K. Sandeen *

AARON COOPER: I think we'll get started back up with the second half of the session. Our next speaker is Professor Sharon Sandeen from Hamline University School of Law. Prior to becoming a full-time professor in 2002, Professor Sandeen practiced law for over fifteen years in Sacramento, California, first as a general business litigator at the largest law firm in Sacramento, and later as an intellectual property specialist where her practice included trademark registration and intellectual property litigation. Professor Sandeen's teaching career began in 1996 when she was appointed as an adjunct professor at the University of Pacific McGeorge School of Law. Since 1996, she has taught an IP survey course at least once a year as well as a variety of other IP courses, including trademark law, copyright law, computer and internet law, trade secret law and international trade secret law.

Professor Sandeen will be speaking on IP protection in the Cloud. So please join in welcoming Professor Sharon Sandeen.

SHARON SANDEEN: Thank you. I am very happy to be here, and one of the things that is great about coming to a conference like this is I learn so much from other people. And, Janet Stiven, your presentation was great, so thank you. I also want to thank the organizers of the symposium for inviting me and my friend Josh Sarnoff, who is one of the IP professors here at DePaul.

I remember coming here for one of the first IP Scholars Conferences in 2004. DePaul is one of the four schools that sponsor that conference every year. Professor Roberta Kwall was very supportive of the young scholars at that conference and talked to us about our scholarships. At that time I had this crazy idea that I was going to focus my scholarship on trade secret law, which for those of you who may not be aware, has not received much attention by the legal academy. But that is starting to change.

I'm going to present in four parts. First, I will talk about intellectual property issues from "meatspace" to online services and the Internet (I will explain what I mean by meatspace in a minute). Then, I will

* Professor of Law, Hamline University School of Law

talk about intellectual property issues from the Internet to the Cloud. Finally, I will discuss the implications of cloud computing for trade secret protection.

There are many legal issues related to the Internet, but I am not going to talk about cyberspace generally. When I refer to the period of "meatspace to the Internet," I am really talking about meatspace to cyberspace. The casebook I cite in my written materials gives a great overview of the issues regarding cyberspace organized around various problems.[1] And many of them have been touched upon already. I will be touching on the problems underlined on the screen. Although I added the one at the bottom, "problems of information security," and I would also add confidentiality. When the commercial use of the Internet started we were really looking at these issues from a point of view of personal privacy and surveillance and not so much concerning the security and legal status of stored data.

I am also not going to address all of the different modalities for solving the problems that we face in cyberspace made famous by Lawrence Lessig's article: The Law of the Horse: What Cyberlaw Might Teach.[2] The four modalities are: (1) the law, (2) social norms, (3) contracts and private ordering, and (4) architecture and the code. So keep that in mind.

As lawyers we have many ways to solve the problems that we are talking about today. I will focus today on the legal solutions with some contractual and practical solutions thrown in. But I want to start with the legal issues of meatspace.[3] I always love coming to Chicago because it is the birthplace of my father and his parents. In fact, my grandmother was born just west of here across the river in 1906, the child of Italian immigrants. She lived in the house on the now destroyed Bunker Street, a stone's throw from Hull House which is depicted in the postcard shown on the screen. It wasn't until many years after I first read Jane Addams' autobiography, Twenty Years at Hull House[4] (which was published in 1910), and after I acquired a map of

1. Patricia L. Bellia, Paul Schiff Berman and David G. Post, CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE, 3d ed. (West 2007) (detailing (1) problems of metaphor and analogy; (2) problems of geography and sovereignty; (3) problems of legal versus technological regulation; (4) problems of "public" versus "private" regulation; (5) problems of speech regulation; (6) problems of intermediaries; (7) problems of privacy and surveillance; (8) problems of information enclosure; and (9) problems of cultural change).

2. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501 (1999).

3. "Meat space" is defined by the Urban Dictionary as "referring to the real (that is, not virtual) world, the world of flesh and blood. somewhat tongue-in-cheek. the opposite of cyberspace." Urban Dictionary, http://www.urbandictionary.com/define.php?term=cyberspace.

4. JANE ADDAMS, TWENTY YEARS AT HULL HOUSE (1910).

the area, that I realized that Jane Addams' book told the story of my family and the many immigrant families like it.

Eighty years after Jane Addams' death I wonder what she would think of the world we live in compared to the problems she dealt with. The meatspace of late 19th century and early 20th century Chicago seems simple and mundane compared to cyberspace and the Cloud of today. If you do not know a lot about Jane Addams, one of the things she did is she complained about the garbage that was being thrown on the streets in the poor areas of Little Italy, and she complained so much to the City of Chicago that they finally appointed her the head of garbage collection. And she fixed that problem. That was one of the things she did.

There is a connection, however, between the problems that Jane Addams encountered in the tangible world depicted in the postcard and the problems we now encounter in the Cloud. With every advance in technology comes a new set of problems to be solved and new legal issues that arise therefrom.

A lot of what I am going to talk about today is based upon personal observations and experiences growing up within a 30-minute drive from the garage made famous [shown on a Power Point slide] by Hewlett Packard. But also Apple Computer was started in a garage too. But what I am talking about is also based upon the experiences practicing law in Sacramento, California between 1985 and 2001 and personally witnessing the transition from old style typewriters to IBM Selectric typewriters, to Wang typewriters, to IBM compatible desktop computers, and finally to laptop computers. And for the students in the audience, the item on the top left of the slide, that is what a typewriter looks like. I used all of those in my law practice in the span of sixteen years. But just imagine the technological changes that Jane Addams experienced during her lifetime: the automobile, the airplane, the telephone and the telegraph, to name just a few examples.

The book, The Victorian Internet, tells the story of the telegraph.[5] In one chapter, the author goes through the legal issues encountered because the telegraph was adopted. So what we are talking about now is not new. Let me give you some examples. What if a message was wrongly entered by the telegraph operator and the company placed an order for one hundred bushels of wheat instead of ten? Who would be responsible for the additional cost? What if a message about a death was mis-delivered by Western Union causing emotional upset?

5. TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS (1998).

Should there be a cause of action? What if the telegraph was used by some enterprising soul to beat the odds of betting on a horse race by getting the results of a horse race before the betting parlors closed their windows? Was a new law needed to outlaw such behavior? Yes, it was; and it was enacted.

Viewing current-day problems involving the Cloud through the lens of history to me suggests two basic approaches to legal issues and then some sub-issues. First, how is the problem the same or similar to problems that we encountered and solved in the past? That is the problem of analogy. Second, how are the problems different from what we encountered in the past, thereby perhaps requiring a different solution? And then based upon recent history involving the Internet, there are important sub-issues and new approaches to those problems. An example of this, of course, is "click to agree" or "browse to agree" terms of service agreements used by most Internet Service Providers (ISPs). One can argue that to allow for the flourishing of the Internet, courts basically did away with the whole concept of mutual assent in contract law. Now for all of those students who are graduating soon and are going to take the Bar Exam, mutual assent is still tested on the Bar Exam, but it is not necessarily enforced on the Internet.

So what are the legal issues regarding the transition from meatspace to the Internet? This is where I am moving to the meaty part of my presentation, pun intended. I want to talk about some of the legal issues that arose when we transitioned from communicating in meatspace, the tangible physical world, to communicating on the Internet. I am talking about pre-cloud now. What is going to emerge out of my talk is an identification of what is different about the Cloud, but we need to understand what was going on when we transitioned online, onto the Internet.

Now next year, April 30, 2015 marks the 20th anniversary of the dismantling of the NSFNET, the Internet backbone service—the government-run Internet.[6] Catherine Sanders Reach mentioned earlier that the Internet is twenty-five years old this year,[7] but I have always marked the beginning date of the Internet when the backbone was taken down because that is when the commercial use of the Internet began to predominate. So next year is the 20th birthday of the In-

6. For a history of NSFNET, see http://www.nsf.gov/about/history/nsf0050/internet/launch.htm and http://www.nsf.gov/about/history/nsf0050/internet/anend.htm.

7. This anniversary actually refers to the twenty-fifth anniversary of the world wide web invented by Sir Tim Berners Lee and dedicated to the world. *See* http://googleblog.blogspot.com/2014/03/on-25th-anniversary-of-web-lets-keep-it.html.

ternet as we know it today, but many of the issues of the Internet that we know today actually started a little bit earlier when pioneering companies like CompuServe, Prodigy, and America Online offered on-line communication services that required the use of, God forbid, telephone modems. So as with the telegraph before it, these modes of communicating and exchanging information raised a host of legal issues.

First, there were a range of issues that arose that were related to the ease with which information that exists in digital form can be copied and shared. Although of most concern to the copyright intensive industries such as the movie industry, the ease with which information could be shared off the Internet raised problems for trademark, patent, and trade secret owners as well. So let me go through some of these issues. First of all, the copyright intensive industries saw the problem right away; and one solution that they came up with was to embed technological protection measures into the digital media to essentially lock down content and make it more difficult to copy. That didn't really work too well mainly because people didn't want to buy stuff with those protection measures. But anticipating that people would try to circumvent these measures, we passed the Digital Millennium Copyright Act in October of 1998.[8] Among other things, the DMCA made it illegal to circumvent such measures.

Efforts were also undertaken at the international level principally through the World Trade Organization, Agreement on Trade-Related aspects of Intellectual Property (also known as the TRIPS Agreement) to increase IP protection worldwide and beef-up IP rights.[9] Those efforts continue.

Another issue that arose concerning copyright issues and defamation issues related to user generated and posted content (sometimes referred to by the acronym "UGC") and the potential liability of Internet service providers for such content with respect to potential copyright infringement. We solved that through a provision of the DMCA that provides safe harbors from copyright liability for Internet service providers that institute a notice and takedown process.[10]

With respect to defamation issues, and now according to some case decisions other forms of potential liability for ISPs, was solved through the enactment of section 230 of the Communications Decency

8. Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

9. *See* Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization (April 15, 1994).

10. 17 U.S.C. § 512.

Act.[11] Another set of copyright issues that arose with the advent of the Internet, but that focuses more on users and purchasers of copyrighted content rather than the producers, concern the extent to which the copyright doctrines of fair use and first sale can be limited or modified by code or contract. And this is what Catherine Sanders Reach referenced earlier when she talked about rent versus own.

When we let other people control information then they might be able to limit our uses of that information in ways that we would normally be allowed to make of that information under the law. This also refers back to the advent of the terms of use agreement and click to agree and browse to agree forms of consent. Many of these agreements modify copyright principles, including the fair use of documents and the first sale doctrine, and related to trade secret law, they often restrict the ability to reverse engineer. These issues, which were first raised with the advent of the Internet, persist with the Cloud.

The trademark issues that arose with respect to the transition from meatspace to the Internet had largely to do with the global nature of the Internet and the increased risk that globalization posed for potential infringement. Just imagine if you adopted a trademark here in Chicago and you put a website up and then somebody in a distant state sees your website and sees your trademark and says, "I think I'll adopt that name for my company." Just the increased access to information about an otherwise local business created an increased risk of trademark infringement. Under U.S. law, before the Internet, that might not be an infringement, particularly if there is no present likelihood of confusion in the relevant markets, because it is legally possible for two or more companies to concurrently use and own the same trademark under certain circumstances.

The other trademark issue that came up had to do with the Internet itself and its domain name system and gave rise to problems concerning the sale and use of domain names that were the same or similar to registered and unregistered trademarks.

As with copyright problems, we addressed the trademark problems in a variety of ways, through refinement of existing law that reshaped the geographical scope of trademark; through the adoption of new laws;[12] and through increased trademark protection effort internationally. Also, with respect to domain name issues, we created a private dispute resolution process known as the uniform domain name dis-

11. 47 U.S.C. § 230.

12. 15 U.S.C. §1125(d) (2012).

pute resolution process, the UDRP.[13] So that solved a lot of those problems.

With respect to the issue of the senior user of a trademark anywhere being the victim of infringement by a junior user and potentially even the registration by a junior user, we created the intent to use system for trademark registration.[14] We expanded or paid more attention to the international concept known as well-known marks which allows well-known marks to trump junior users in some cases.[15] We adopted the federal law to protect famous marks known as the Federal Trademark Dilution Act,[16] and we also enacted the anti-cyber squatting law to address the worst kinds of domain name problems.[17]

There were not a lot of patent issues that arose from the transition from meatspace to online services and the Internet unless you include the issues surrounding the patentability of software and business methods. Those are big issues, obviously, but focusing on the communicative and storage aspects of the Internet, there were not many issues; but there is a practical effect related to patents, and that is the *de facto* broadening of prior art because more prior art is now accessible via the Internet.

For those of you who are not familiar with patent law, you cannot get a patent unless the invention has not been invented earlier. The evidence we look for to figure out if an invention has been invented earlier is known as prior art. One of the best forms of prior art is previously published information. The more inventions that are documented and stored in a manner that makes them accessible to others, the more prior art there is; and, in theory, the less patents will be issued.

Now, obviously, the Internet increased the volume of both stored and accessible information, with all sorts of things and all sorts of inventions being capable of being found during a prior art search; and if your client is sued for patent infringement, I suggest you look at that information because it might provide a useful defense.

That brings me to trade secret issues. The trade secret issues that arose with respect to the transition from meatspace to the Internet are very similar to some of the copyright issues I mentioned earlier. With the advent of the computer industry, computer storage and the Internet, it became a whole lot easier to misappropriate trade secrets.

13. *See* http://www.icann.org/en/help/dndr/udrp.
14. Pub. L. 100-667, 102 Stat. 3935 (1994) (codified in section of 15 U.S.C. § 1051(b)).
15. *See* TRIPS Agreement, Articles 16.2 and 16.3.
16. Pub. L. No. 104-98, 109 Stat. 985 (1996) (codified at 15 U.S.C. §§ 1125(c), 1127)
17. *See* note 12 *supra*.

In Jane Addams' day, up through the first use of magnetic tape to record computer data in 1951, information was usually stored in filing cabinets and bankers' boxes. In order to engage in reasonable efforts to maintain the secrecy of information which, as I will explain in a moment is a key for trade secret protection, one just needed a good lock or perhaps a series of locks or a vault. Anyone who wanted to misappropriate information would have to either gain access to it rightfully and then breach a trust imposed on him or break and enter the locked facility.

The storage of information has changed a lot since my first real job in 1973 as a file clerk. It has gone from locked rooms, file cabinets and bankers' boxes to magnetic tape, hard drives, floppy disks, jump drives or some combination of the foregoing. With the advent of the Internet, trade secret experts and scholars pointed out that businesses had to pay closer attention to the various forms of document storage and make sure to secure their trade secrets wherever they may reside.[18] The same is true today with the Cloud.

For computer media this might include the use of passwords, firewalls, encryption and other digital security measures. It should also include better employment and business practices that require express confidentiality agreements and that limit who can have access to the trade secrets. It should also include increased monitoring and policing of downloading activity, particularly (and, I should add, with respect to the Cloud, uploading activity) with respect to disgruntled employees and computer hackers.

And commenting on what Janet Stiven and Catherine Sanders Reach talked about, the standards of security, there is an unresolved issue whether meeting a particular security standard also meets the reasonable efforts requirement under trade secret law. (If you remember from tort law, particularly for those in the audience who are taking the Bar Exam this summer, generally speaking we do not let industry standards set the "reasonable man" standard.)

The statutory solutions to these problems included the enactment of the Computer Fraud & Abuse Act to outlaw computer hacking activity,[19] which is still the law, and the Stored Communication Act which makes it illegal for electronic communication services and remote computing services to "knowingly divulge information stored by their customers."[20] (As I will explain in a little bit, that is a very narrow

18. See e.g., Victoria Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 3 INTELL. PROP. L. REV. 359 (2009).

19. 18 U.S.C. § 1030.

20. 18 U.S.C. § 2701–2712.

statute and was actually adopted before the commercial use of the Internet began.)

So what are the issues from the Internet to the Cloud? And I should say the Cloud is roughly nine years old. Rack Space claimed to have actually invented the idea in 2005, and Dell actually tried to trademark (or register) the term as a trademark in 2006. The copyright and trademark issues are not that much different because of what Catherine said earlier, that the Cloud is a metaphor for the Internet anyway.

With respect to the ease of copying and the global reach of communications cloud-based business models may magnify the copyright and trademark problems that I just discussed, but I don't think they give rise to many new or different problems except for the following.[21] I think there are likely to be more complex copyright and invention ownership issues with respect to works of authorship and inventions that are collaboratively created using Cloud services because a lot of these services offer an opportunity for people to collaborate in the Cloud. If new works of authorship happen to be collaboratively created by the employees of the same company, then you are in luck because at least in the United States the work for hire doctrine will apply and the rights in such collaborative work will belong to the employer.[22] However, the Cloud is bound to complicate the analysis because the collaborators may be located in different countries, and most other countries do not have a work for hire doctrine. So that will not apply in those countries.

Most other countries, like the U.S., have a default rule that whoever the creator is owns the copyrights. If the collaboration involves independent contractors or the employees of other companies, the copyright ownership issues will get really messy, similar to the problems that movie production companies face. (But in the case of movie production companies, under U.S. law there is a statutory provision which makes those collaborations potentially works for hire because there is a statutory work for hire category under the independent contractor prong for movies.[23]) Now this is true of inventions that are created through collaborative processes as well.

---

21. The *Aereo* case that was recently heard by the U.S. Supreme Court raised the issue (or fear) that a broad definition of the public performance right under U.S. copyright law would adversely affect Cloud providers if their storage of copyrighted works uploaded by customers was considered a public performance. *See Am. Broadcasting Cos., Inc. v. Aereo, Inc.*, 573 U.S.__ (2014).

22. 17 U.S.C. § 101 (defining of work made for hire).

23. Id.

The resolution to this problem is to deal with the ownership issues up front by getting all collaborators to execute an agreement that spells out who owns what. But this may be difficult to do without policies about who can participate in such collaboration. The other option is to adopt an innovation model that may or may not include dedicating the work of authorship or invention to the public domain. In other words, if a company is going to use a collaboration model using the Cloud, they might want to just say: "Whatever is produced in the Cloud is going to be dedicated to the public domain."

Turning to the patent and trade secret issues, as noted previously, there were not many patent issues that arose due to the communicative and storage aspects of the Internet; but I will lump patents and trade secret together for the rest of my discussion because the invention that may be the subject of a patent application always begins as a trade secret, or at least one would hope so.

The status of information stored in the Cloud, and whether it is disclosed by the mere act of storage, raises concerns not only for the potential waiver of trade secrecy but for the loss of potential patent rights. This could happen in two ways. Internationally, certain public disclosures constitute prior art which then bar patentability for what has been disclosed in a given country. In the United States, certain disclosures trigger a one-year grace period in which to file a patent application.[24] So it is important to know if and under what circumstances the storage of trade secrets and information regarding patentable inventions constitutes the disclosure for both trade secret and patent purposes.[25]

From a patent point of view, the analysis is complicated by recent amendments to the U.S. patent law which change the statutory definition of prior art under section 102 of the Patent Act. Some people argue that the new definition did not change old law that much and certainly did not narrow the meaning of disclosure that triggered a one-year grace period.[26] Others argue that the meaning of disclosure was narrowed in significant respects.[27]

How this debate plays out remains to be seen. For present purposes, the key issues are: (1) Does storing information in the Cloud

24. 35 U.S.C. § 102(b).

25. See Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, forthcoming in the Virginia Journal of Law & Technology.

26. Robert P. Merges, *Priority and Novelty Under the AIA*, 27 BERKELEY TECH. L. J. 1023 (2012).

27. Robert A. Armitage, *Understanding the America Invents Act and Its Implications for Patenting*, 40 AIPLA Quarterly 1 (2012).

constitute a disclosure under any current or possible future meaning of that term under either patent law and trade secret law?; (2) If so, is there a way to differentiate between potentially trade secret and patent destroying disclosures and something else?; and (3) Does it depend on how and where information is stored?

I am going to address these issues as they relate to trade secrets, but first a little trade secret 101.[28] I am not sure if everyone is familiar with trade secret law, but essentially the predominant law governing trade secrets in the United States is the Uniform Trade Secret Act. It is now applicable in forty-seven states. The only three states that do not follow it are Massachusetts, New York, and North Carolina. However, in North Carolina they have a statute for trade secret protection. It was just adopted before the Uniform Trade Secret Act, so it is not counted as a Uniform Trade Secrets Act state.

It is very clear that there are two basic elements of a trade secret misappropriation claim. First, you have to have a trade secret, and, second, it has to be misappropriated. Importantly, under the definition of a trade secret there are three requirements: secrecy; independent economic value; and reasonable efforts to maintain secrecy. If you have those three, you have a trade secret.

With regard to misappropriation, the statute is very convoluted in describing what constitutes a misappropriation, but if you read it carefully, it basically breaks it down into what I have on the screen. First, it is wrong to acquire trade secrets by improper means. Second, it is wrong to disclose or use trade secrets in violation of a duty of confidentiality. Now at this point you may be asking yourself how the evolution from the online services of old without a focus on cloud computing to the current Internet with a focus on cloud computing presents different issues with respect to trade secrets. In other words, why have these issues not come up before when bankers' boxes were stored off-site or when companies used back-up services to store data, which is something that has been happening for decades?

Admittedly, like all good attorneys and scholars should do when faced with new technology and new methods of doing business, I am trying to anticipate problems and provide a potential solution before they become pervasive. So let me explain why with respect to trade secrets I think things may be different in the Cloud versus earlier methods of storing information. A lot of what I'm going to say has already been covered but it will be good to review.

---

28. *See generally* SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW IN A NUTSHELL (2013).

First, the information is stored remotely. There is, of course, historical precedent for this both in meatspace during the computer time-sharing era of the 1960s, 1970s, and the pre-Cloud days, but I think things are different in the Cloud because the nature and amount of information being stored is greater. It is also different because the relationship between the information owner and the Cloud storage service is different.

That leads me to my next point: the information is transmitted and accessed over the Internet. Now old methods of off-site storage, even in the early days of main frames and mini computers, often involved the transfer of information in tangible form through the use of couriers. With those big magnetic tapes, a picture of which I showed you earlier, a human being would actually carry a magnetic tape from point A to point B. This did not allow for computer hacking because nothing was being transmitted electronically.

In the early days of online services on the Internet, even if things were transmitted electronically, it was a transient one-time deal. Information would be transmitted from point A and point B and then stored until accessed or transferred back at a later time, hopefully with the use of a password and an encryption key, and often over a private network. Thus, although the act of initiating back-up storage could involve the Internet or a private network, what is different about Cloud storage services is the on-demand, self-service and broad network access that the National Institute of Standards & Technology says are central characteristics of cloud computing. In other words, there is a constant ability to access the information. It has already been mentioned that the computer servers can be located any place in the world. This is not true with respect to cabinet files and bankers' boxes. Even if you wanted to store things off-site, you would pick a company that was close to your place of business in case you had to access that information at a later date.

In the early days of online services and the Internet, electronic storage might be remote, but usually at one server farm in one physical location where you knew its location. What is different about modern Cloud storage services, unless the companies are willing to contractually agree to geographic restrictions, is that stored information may flow to different servers located in different places around the world depending upon the available server capacity. In fact, that is the scalable feature of the Cloud and cloud storage. It is one of the key features of the Cloud.

Another important point is that information can be accessed anywhere in the world, and so the point is: How do you monitor and

police that? Let me explain that in meatspace, based upon a number of trade secret cases, if you wanted to present evidence of misappropriation, often times it went something like this: "I saw so and so coming to the office late at night when he does not normally come to the office late night, and he left with a big bankers' box of, I don't know what, which he doesn't normally do." When we went online on the Internet—in the early days of the Internet or digital means of storage—the evidence would be something like: "I saw so and so late at night in the office downloading stuff onto a jump drive or a floppy disk." What you have now with the Cloud is that the "so and so" who could be misappropriating something could be sitting anywhere in the world and they could be an employee of a company, become disgruntled, take a trip to China, decide to download—does this sound familiar? It sounds like Edward Snowden, doesn't it?

So it is not just the downloading activity that you have to monitor but the uploading activity as well. Unfortunately, Cloud computing companies are reticent to agree to any obligation of security or confidentiality. Since I started to write a paper on this topic—I think it was in 2009—the Cloud computing contracts have definitely evolved, particularly because of the work of attorneys like Janet Stiven saying "you shall do this," more companies are willing to perhaps agree to certain things.

But generally speaking, they disclaim any duty of confidentiality, any security, any liability, et cetera. In fact, I have been hard pressed to even find the word "confidentiality" in any of these agreements. They will talk about privacy and security, but they will not necessarily talk about confidentiality. I will explain in a minute why that makes a difference with respect to trade secret law.

But I find all of this ironic because Cloud computing companies and Cloud storage services are touted as alternatives to a back-up service when in reality companies still need back-up services. Now they have to back up everything that is stored in the Cloud as well as everything that they store on their own in-house servers. So this goes to the point that Janet Stiven made: you have to figure out the real cost factors.

Finally, some cloud storage services are not passive storers of information; and this is of great importance for those who may argue that these services are remote computing services that are required by the Stored Communication Act not to knowingly divulge information stored by customers.[29] There are a lot of exceptions and nuances to

29. 18 U.S.C. § 2701–2712.

the Stored Communication Act, but let me just go through a few reasons why I think it might not apply to the Cloud.

First, the requirement does not apply to services where the provider is authorized to access the content. And, by the way, Google, for instance, is a company that reserves the right to access its customer's content. Second, it only applies to services provided to the public. Thus, so-called private Clouds and hybrid Clouds, depending on how they are set up, may not count.

Next, if the information is being stored outside the United States, even if the Stored Communication Act applies, does it apply to data that is stored outside of the United States? I would guess not. There is also an issue of whether or not cloud storage services meet the statutory definition of a "remote computing service."

And then, finally—and this is more of a legal question—even if the Stored Communication Act requirements apply, there is a legal question of whether it imposes a duty of confidentiality for trade secret purposes as opposed to a legal duty not to knowingly divulge. I would argue that the two are different.

So what is the problem? The problem is what I have labeled "the third-party doctrine of trade secret law."[30] I used that label because it is very similar to the third-party doctrine of Fourth Amendment jurisprudence. This longstanding doctrine states that if a trade secret owner voluntarily discloses trade secrets to another who is not under a duty of confidentiality, then the trade secrets are waived. The reason it is called the third-party doctrine is because another party (other than the third party) is usually the party to the litigation.

What you do as a defendant in a trade secret misappropriation case is you ask the plaintiff: Where did you keep your stuff? If they say "I kept it in the Cloud," then you argue they waived trade secret protection. Now the important thing here—and there is some debate about this, but I think I am right—is that you waive protection even if the information does not become generally known or readily ascertainable. And the reason I think I am right is because of the notice function of the reasonable efforts requirement of trade secrecy. If we did not interpret trade secret law this way, the reasonable efforts requirements would be meaningless; and the reasonable efforts requirements cannot be meaningless because that is the notice function of trade secret law.

We do not want people to go to work at some place or to deal with information and then be sued for trade secret misappropriation and

30. *See* Sandeen, *supra* note 25.

have them say: "I never knew they were trade secrets: I never knew I had an obligation." We may want to say it does not matter, but that is how trade secret law is different from trademark, copyright, and patent law. Trademark, copyright, and patent claims are more like strict liability torts. Under trade secret law there is a knowledge element and, in turn, the need for a duty of confidentiality serves the reasonable efforts requirement.[31]

So let me expand on this point. As I previously mentioned, Cloud storage services are generally unwilling to enter an express confidentiality agreement. Without such an agreement trade secret owners might rely upon implied agreements, if any. However, the terms of service agreements used by cloud storage services (and I might add not just terms of service, but privacy policies and all the other provisions) typically contain disclaimers of relationship, duties, and liabilities. If you remember from contract law, this makes it difficult to prove an implied duty of confidentiality since a well-established rule of contract law is that you cannot imply an agreement if it is expressly disclaimed.

Of course there may be issues regarding the actual language of a particular terms of use agreement, but there is plenty of language in most of them that express a disclaimer of security and confidentiality. So if you cannot prove an implied-in-fact agreement, the only argument left is that an implied-at-law agreement of confidentiality was created. But the nature of the disclosure will make it difficult to have an implied-at-law confidentiality agreement.

Case law suggests that an implied-at-law confidentiality agreement does not arise unless at least two things happen. First, the recipient of the information has to know that the information contains trade secrets. Second, it has to be reasonable to assume that the recipient of the trade secrets knew that they were to be kept in confidence. Merely transferring trade secrets to another is not enough to create a duty of confidentiality. You cannot unilaterally create a duty of confidentiality.

So what are the solutions? First, do not put trade secrets in the Cloud, period. One reason for this is not only because of the effect of the third-party doctrine on trade secrecy, but also because you have to understand that every time you share trade secrets with another, whether you have a duty of confidentiality or not, it creates two levels of reasonable efforts requirements. You have to met the reasonable effort requirements at your own facility, and you have to make sure

31. See UTSA section 1 (defining misappropriation).

that reasonable efforts are instituted at the other's facilities as well. It just so happens that getting an express duty of confidentiality from the third party is evidence of reasonable efforts, but arguably it is not enough alone. If you have to put information in the Cloud, segregate the trade secrets from other information and put them in a more private and secure place, like a private Cloud or a better-encrypted part of the Cloud. Segregate the trade secrets from the rest of the information.

Also, be sure to exact an express promise of confidentiality, if possible.; and I am emphasizing the word "confidential," not security and not privacy. Confidentiality. That is the key.

If you cannot get an express promise of confidentiality, then you are going to have to rely on an implied-at-law theory. I would not recommend this because it is hard to prove, but to increase your chances, mark all legitimate trade secrets as confidential and inform the cloud storage service that you are doing so.

Now, I was joking with Professor Sarnoff that we should have a battle of the terms of use agreements since mutual assent is so easy or nonexistent when the Internet service provider and Cloud providers enter in to a contract with everybody, including all of us and our clients. We should just turn the tables on them—when you submit information to the Cloud, include a statement that reads "by accepting this information for storage you hereby agree to keep it confidential." I do not know if that would work, but it would show the irony of changing the law for one industry and not understanding that such a change might impact another.

With regard to the issue of an implied-at-law duty of confidentiality, ask yourself if we want such an implied duty of confidentiality to attach so easily because the loosening of existing standards may be applied to you and your client in other non-cloud contexts. The place where this comes up a lot in trade secret law is with respect to idea submission claims, where somebody has an idea and they run off to a big company and say "here's my idea." Then, a year or so later, the company starts using that idea and they get sued for misappropriation. There have been plaintiffs in that situation who have been successful in proving an implied-at-law duty in confidentiality, but, generally speaking, the courts do not like the idea of people unilaterally exposing their ideas to companies and then suing them. If we lower the standards for creating an implied-at-law duty of confidentiality for purposes of the Cloud, it whould be lowered for all other industries, and that is a problem.

From a legal perspective, here is what I propose instead. We need a new or expanded taxonomy that differentiates between disclosures and mere transfers. In the paper I just finished, I detail the differences.[32] But generally, the definition of disclosure I propose has to do with whether knowledge has actually been transferred to a human being in a way that the human being is conscious of it. It may be that for a lot of what is going on in the Cloud, knowledge transfer is not happening, and, therefore, it would be a "mere transfer." But some companies are accessing information stored in the Cloud and reading it and using it; knowledge is being transferred. Other situations would not involve a knowledge transfer, and I argue that if it is a mere transfer it should not waive trade secret protection.

Finally, perhaps we should amend the Stored Communication Act to create some sort of statutory duty of confidentiality under certain conditions; in this regard I might point out that even though there are always laws regarding security and so forth, it is ironic that the companies still disclaim responsibility even though they have a legal duty of security under a number of provisions of law. I do not propose bending and stretching existing laws to help the Cloud and Internet industries. Unlike the early days of the Internet, I think the players can afford to separately negotiate contracts or otherwise make express duties of confidentiality or security; and, more importantly, I think it is good public policy that we insist that they do so.

Thank you for your attention. I ended with a picture of Jane Addams in case you did not know what she looks like.

AUDIENCE MEMBER: If I take my trade secret documents down to my local bank and lock them in the lock box at the bank, I do not think I have run into a problem with a trade secret disclosure doctrine. If I investigate the security of a Cloud storage company and they make certain representations that they have certain levels of security, why is that any different if I store my documents there?

SHARON SANDEEN: That might explain why recently a very enterprising journalist called me because he had this idea that if we stored stuff in the Cloud that certain Fourth Amendment and trade secret rights would be destroyed. I explained my theory, and when you talk to a reporter for a half an hour they use only one sentence. I think the sentence this reporter used was something like, "if you store it in the cloud you're going to lose these protections." The story got picked up by the ABA, and somebody on their blog wrote: "That's the most idiotic thing I ever heard." So here's the thing. I know what

32. *See* Sandeen, *supra* note 25.

people want the result to be, but there is no existing case law that supports it. And so that is why I am proposing a new taxonomy that would allow us to solve this problem in the way that people have an instinct about how it should be resolved. And the point is that we do not have a clear understanding under the law of what disclosure means, and we do not differentiate between disclosure as a transfer of knowledge and the mere transfer of information. So I think your instincts are right, but I think there are situations where there is going to be a transfer of knowledge, and that is the problem.

AUDIENCE MEMBER: Would it protect a trade secret if the Cloud computing service would agree to reasonable efforts to keep it confidential or to keep it secure?

SHARON SANDEEN: A common strategy in contracts involving the licensing of trade secrets is to impose on the other party a duty to engage in reasonable efforts. If I were advising a client, putting that clause in a contract would not be enough. Because what are they going to actually do? Sometimes what attorneys do is say you must engage in reasonable efforts that are at least as good as the reasonable efforts that we engage in, but there is no specificity about what that is either. Because reasonable efforts is a very fact specific analysis, and because you can lose trade secret rights if you don't get it correct, my advice is to do more than just put that in the contract. You need to specify who has access to the information, under what circumstances, where it is kept in the meantime, and so forth.